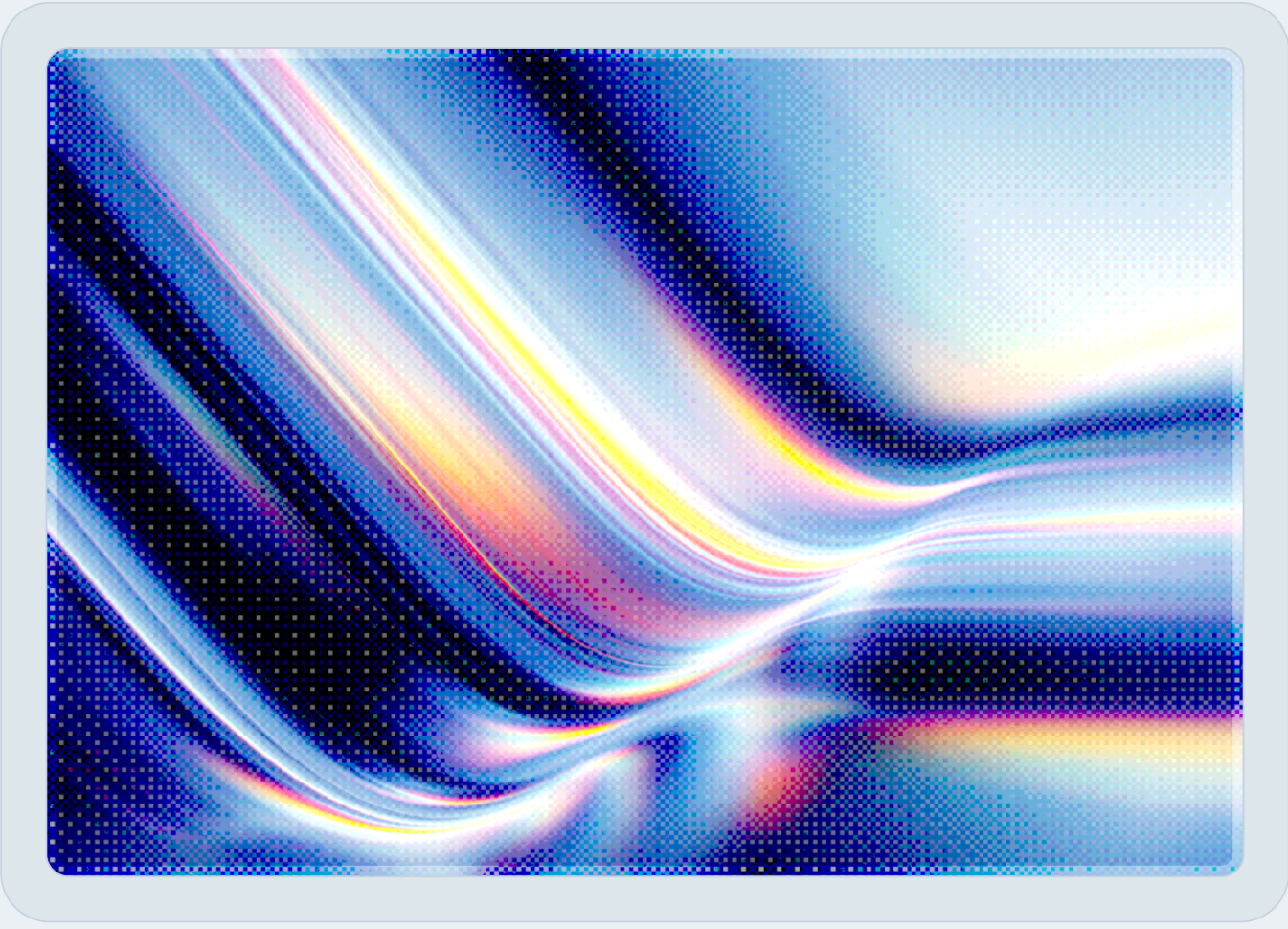
CSAI Foundation | Cloud Security Alliance

Up to Fifty Ships: Maritime Cyber Campaigns and Edge-Device Concentration

Geopolitical Spillover into Supply Chains: Security Implications and Guidance

2026-11-28

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

U.S. officials are investigating intelligence suggesting that up to 50 commercial vessels, many carrying oil, liquefied gas, and chemicals, were compromised in a cyber campaign that federal officials suspect may be linked to Iran [1][2]. The figure is an unofficial intelligence estimate, not a confirmed count, and no government has publicly attributed the activity [2]. What has been confirmed is narrower but still significant. The FBI and U.S. Coast Guard boarded two inbound foreign-flagged vessels in August 2026 after detecting network compromise. In September they issued a maritime cyber alert warning that threat actors were exploiting Fortinet FortiGate firewall and VPN devices across the marine transportation system [1][3][4].

The reported intrusion path matters more than the headline number. According to a U.S. official quoted by NPR, attackers used known FortiGate weaknesses to get in, then pivoted from shipboard IT networks into operational technology (OT) that "could have impacted" propulsion, steering, navigation, and cargo management, although no such manipulation has been publicly documented [1]. The official described the attacks as "not sophisticated" and said they could have been mitigated through basic cyber hygiene [1]. The campaign follows the June 2026 FortiBleed credential exposure, which CISA tied to roughly 74,000 Fortinet devices [7]. Trade press reporting on the September alert says it cited CISA's FortiBleed figures and that the campaign "tracks closely" with FortiBleed credential harvesting [3]. No public source has confirmed that FortiBleed credentials were the entry point on any specific vessel, but the leak shows how one exposure event can reach a large share of an installed base at once.

For enterprises outside shipping, the lesson concerns structure more than sector. When the same perimeter appliance guards many of a sector's remote assets, a single credential leak or vulnerability becomes a fleet-wide exposure. Geopolitical conflict can then turn that latent exposure into operational risk quickly. Organizations that depend on maritime logistics, or that run remote OT behind commodity edge devices, should treat this campaign as a live test of their own resilience.

Background

The campaign sits inside an unusually hostile maritime environment. The 2026 U.S.–Iran conflict began in late February, and the United States imposed a naval blockade on shipping to and from Iran on April 13, 2026. The blockade was lifted after a June peace memorandum, then reinstated on July 14, 2026, and it

has produced repeated seizures, diversions, and boardings of commercial vessels [10]. Commercial operators have faced electronic interference at the same time, as maritime security reporting describes spoofed GNSS positions being rebroadcast over AIS as a growing hazard to shipping [4]. NPR reports that U.S. experts and officials also suspect Iranian hackers in attacks on U.S. water treatment systems in August and on commercial refrigeration systems in early November. That pattern suggests civilian infrastructure is among the target set in the conflict [1].

The confirmed maritime incidents began in August. On August 21, 2026, a multi-agency team that included a Coast Guard Cyber Protection Team and the FBI Cyber Action Team boarded the first of two inbound foreign-flagged commercial vessels in the Gulf of Mexico. A second team boarded another vessel three days later [3][4]. The FBI and Coast Guard reported no operational disruption, vessel instability, danger to crews, or environmental impact [1][3]. NPR reports that crew members and employees noticed email disruptions or could not log in [1]. One of the boarded ships has been linked to the Liberian-flagged crude carrier VL Prosperity, bound for Galveston; its manager, HMM Ocean Service, confirmed the Coast Guard boarding [5]. That vessel reportedly lost communications for more than 30 hours after an intrusion around the Strait of Gibraltar in early August [5][6]. Iranian state media claimed that attackers took control of the tanker's propulsion, navigation, and cargo systems. Independent analysts have noted that Iranian coverage does not establish responsibility, and that GNSS interference in the Gibraltar corridor could plausibly explain part of the communications outage [5].

On September 4, 2026, Coast Guard Cyber Command and the FBI issued a Maritime Cyber Alert. It warned that nation-state threat actors were exploiting FortiGate devices on vessels and facilities, using compromised credentials, brute force, and vulnerabilities followed by lateral movement, privilege escalation, and persistence [3][4]. The broader picture emerged in late November, when the Wall Street Journal and then NPR reported the estimate of up to 50 compromised vessels, at least one of them an LNG carrier [1][2]. Aggregated reporting citing the Wall Street Journal indicates the affected ships were concentrated in European and Asian waters, and that the Coast Guard deployed cyber protection teams to at least four vessels approaching U.S. ports [6]. That figure counts cyber team deployments; the two August boardings are the cases in which officials have publicly confirmed network compromise [1][3]. A former Navy official told NPR that the government had tracked the possibility of exploiting OT on merchant ships "for a long time" [1].

The table below separates what has been officially confirmed from what remains reported or claimed, a distinction that matters for anyone using this campaign to justify risk decisions.

Claim	Status	Source basis
Two foreign-flagged vessels boarded by FBI/USCG teams in	Confirmed by FBI and USCG	Official statement via NPR [1]; trade press [3][4]

Claim	Status	Source basis
August 2026		
September 2026 alert on FortiGate exploitation in the maritime sector	Confirmed	FBI/USCG alert as reported [1][3][4]
No operational disruption, instability, crew danger, or environmental impact	Official position	FBI/USCG statement [1]
Up to 50 vessels compromised	Unofficial intelligence estimate	Unnamed U.S. official, WSJ and NPR reporting [1][2]
Pivot from shipboard IT to OT networks	Reported by an unnamed U.S. official	NPR [1]
Use of FortiBleed credentials against specific vessels	Not confirmed; alert reportedly cited FortiBleed figures	Cyber Press [3]
Takeover of VL Prosperity propulsion, navigation, and cargo systems	Claimed by Iranian state media; not independently verified	ClearanceJobs, Mallory [5] [6]
Iranian responsibility	Under investigation; not publicly attributed	NPR, Cyber Security News [1][2]

Security Analysis

Edge-Device Concentration as a Fleet-Wide Attack Surface

A central technical feature of this campaign is how much access the attackers reached through how little effort. NPR's source described FortiGate devices as "frequently used in the maritime industry," where they help manage firewalls and virtual private networks [1]. On a typical vessel, perimeter appliances of this kind do a lot of work. They commonly sit behind VSAT, cellular, and Wi-Fi links, broker vendor remote

access, and enforce whatever separation exists between crew, business, and engineering networks. No public data quantifies Fortinet's share of shipboard perimeter deployments. Where one product family fills the perimeter role across many vessels, however, a weakness in that product becomes a sector-level problem. The usual idea of per-organization risk breaks down, because attackers can scan, triage, and exploit the whole population at once. An attacker no longer has to study a particular shipping company's defenses; it is enough to know which appliance the company most likely runs.

FortiBleed shows how quickly that kind of concentration can be exploited. On June 18, 2026, CISA warned that attackers were using compromised credentials against internet-facing Fortinet devices, with leaked credentials tied to approximately 74,000 firewalls and VPN gateways [7]. Based on one researcher's Shodan polling, as reported by Security Affairs, the exposed dataset covered roughly half of the Fortinet firewalls then facing the internet, with management interfaces exposed in most cases [8]. The same reporting noted that many devices still stored administrator credentials as salted SHA-256 hashes, vulnerable to offline cracking from a stolen configuration file, because stronger PBKDF2 hashing takes effect only after an administrator logs in following a firmware update [8]. A credential exposure measured in tens of thousands of devices therefore has a long tail. Rotating passwords helps only if hashes are also upgraded and every device is accounted for. In maritime settings, that inventory problem is compounded by intermittent connectivity and long intervals between port calls.

This is not the first time a shared component has turned many ships into a single target. In August 2025, the hacktivist group Lab Dookhtegan claimed to have disrupted communications on 60 vessels operated by sanctioned Iranian carriers NITC and IRISL by compromising their common satellite communications provider, Fannava. Published screenshots showed root access on Linux terminals running outdated iDirect satellite software, and storage partitions on each vessel were reportedly wiped, leaving every ship needing a full reinstall [9]. The two campaigns sit on opposite sides of the current conflict, and their concentration mechanisms differ. In the Lab Dookhtegan case, one service provider's infrastructure was the single point of compromise; in the FortiGate campaign, the common factor is a product installed independently by many operators. In both, however, one shared dependency became the path to a whole fleet. The table below summarizes these concentration points and their fleet-level consequences; the FortiBleed entry is an illustrative exposure event rather than a confirmed vector in this campaign.

Concentration point	Example	Fleet-level consequence
Perimeter appliance family	FortiGate firewalls and VPNs in the 2026 maritime campaign [1][3]; FortiBleed credential exposure as an illustrative exposure event [7][8]	One credential leak or CVE maps to many vessels and operators simultaneously

Concentration point	Example	Fleet-level consequence
Satellite communications provider	Compromise of a shared satcom provider serving Iranian fleets, 2025 [9]	Single intrusion disables communications across dozens of ships
Legacy terminal software	Outdated iDirect software on vessel terminals [9]	Known, unpatched weaknesses replicated fleet-wide
Vendor remote access	Long-lived vendor VPN tunnels and unexpected connected devices [4]	Third-party pathways bypass operator-managed controls

IT-to-OT Pivot and the Limits of Onboard Segmentation

The reported pivot from IT into OT reflects a well-documented gap in shipboard architecture. CyberOwl, which sells vessel network monitoring, reports from its own telemetry that backdoor or remote-access malware makes up more than 60 percent of the malware it detects aboard ships. It has observed engine-room business computers with two network interfaces bridging networks, misconfigured firewall rules, systems placed on crew Wi-Fi, and as many as 20 unexpected connected devices on a single vessel [4]. Coast Guard Cyber Command's annual reporting, as summarized by The Maritime Executive, shows the same trend from the defender's side. OT was involved in 62 percent of its 2025 cyber missions, up from 46 percent, and phishing achieved initial access in 53 percent of red-team attempts [4]. In such an environment, a compromised perimeter appliance hands the attacker a starting point from which OT reachability is, on many vessels, likely rather than exceptional.

Regulation has not yet closed the gap for the vessels most affected. The International Association of Classification Societies' Unified Requirements E26 and E27 set cyber resilience requirements for ships and onboard computer-based systems, but they apply only to vessels contracted for construction on or after July 1, 2024. Most of today's trading fleet is therefore outside their scope [3][13]. The U.S. Coast Guard's final rule on cybersecurity in the marine transportation system, published in January 2025, phases in cybersecurity plan and incident reporting obligations for U.S.-flagged vessels and regulated facilities; it took effect in July 2025, with cybersecurity plan deadlines falling later [12]. The compromised ships discussed here were foreign-flagged, which leaves port-state boardings and voluntary industry action as the main levers for U.S. authorities [1][3].

Geopolitical Spillover into Commercial Supply Chains

The blockade context changes how this campaign should be read. Military operations at sea have already produced seizures and diversions [10], and spoofed GNSS and AIS data add electronic interference on top of physical risk [4]. If the activity is state-directed, as investigators suspect but have not confirmed, intrusions into tankers bound for U.S. ports fit a strategy of imposing costs on U.S.-linked commercial shipping better than they fit isolated criminal activity. One analyst characterized the early activity as "a rehearsal, not a performance" [5]. That reading is an inference rather than an established fact, but it is consistent with the reported pattern. Access appears to have been gained broadly and used sparingly, and the most visible effects, a communications blackout and email disruption, fell well short of the physical damage the access may have permitted [1][5].

The supply chain implications follow from cargo type and timing. A compromised LNG or chemical carrier raises potential safety concerns. NPR's source said the OT networks the attackers reached could have affected cargo management [1], and on gas and chemical carriers, cargo-handling systems govern temperature- and pressure-sensitive operations. Whether safety-instrumented systems were reachable has not been reported. Short of a safety incident, the operational cost of suspected compromise is substantial in its own right. Boardings, forensic examination, and port-entry delays affect delivery schedules, and the Coast Guard has said it expects to investigate any potentially compromised ship entering U.S. ports during the winter peak [1]. Enterprises that rely on just-in-time maritime logistics may therefore feel the campaign first as delayed shipments, and should watch for knock-on effects such as higher insurance costs, long before any ship's systems are manipulated.

Relevance to AI-Enabled Operations

The campaign also carries a lesson for organizations deploying AI-driven monitoring and autonomous operations at the edge. Vessel operators are adopting remote monitoring, predictive maintenance, and analytics platforms that rely on the same satellite links and perimeter appliances attackers are now exploiting. An AI system that ingests telemetry from a compromised network may be making decisions from manipulated inputs, and spoofed GNSS positions are already being rebroadcast over AIS [4]. Any agent or automation with write access to OT inherits the trust boundary of the edge device in front of it. In CSA's assessment, securing the perimeter appliance is therefore a precondition for trustworthy AI-assisted operations, not a separate concern.

Recommendations

Immediate Actions

Organizations operating vessels, port facilities, or remote OT sites behind Fortinet appliances should act on the FBI/USCG and CISA guidance now, whether or not they have observed an intrusion. CISA's guidance calls for terminating active SSL VPN and administrative sessions, resetting all Fortinet VPN and administrator credentials, confirming that administrator passwords are stored with PBKDF2, and removing unknown accounts [7][8]. The FBI/USCG alert adds patching, credential resets, and log review [3]. Teams should review firewall, VPN, authentication, and domain controller logs for unusual access, rogue administrator accounts, and configuration changes. If unexpected administrative logins appear, the device should be treated as compromised and replacement considered [8]. Management interfaces should be removed from the public internet, and phishing-resistant MFA should be enforced on every remote-access and administrative path [3][7].

Enterprises that ship goods by sea should also contact their principal carriers and freight forwarders promptly. The questions are practical. Has the carrier assessed its fleet against the September alert? Can it confirm IT/OT segmentation on vessels carrying the enterprise's cargo? How will it communicate delays caused by cyber inspections? Carriers that cannot answer with evidence warrant closer third-party risk scrutiny.

Short-Term Mitigations

Over the next one to three months, operators should build an authoritative inventory of edge devices across every remote asset, including make, model, firmware version, management exposure, and credential storage method. That inventory makes the concentration risk visible. Segmentation between business networks and OT should be verified on each vessel, not assumed from design documents, using an approach such as CSA's Zero Trust Microsegmentation Guidance [18]. CyberOwl's findings on dual-homed machines and crew Wi-Fi bridging show how often deployed reality departs from intent [4]. Vendor remote access should move from standing VPN tunnels to time-limited, brokered sessions that are logged and approved per use. Unsupported equipment should be scheduled for replacement, as the FBI/USCG alert recommends [3].

Operators should also apply the joint Five Eyes guidance on edge devices, which treats firewalls, VPN gateways, and routers as high-value targets requiring centralized logging, strict management-plane isolation, and timely patching [11]. For satellite terminals and other maritime-specific edge equipment, the

same principles apply even where vendors have been slow to adopt them, as the outdated terminal software in the 2025 Iranian fleet incident illustrates [9].

Strategic Considerations

At the board and procurement level, the central question is whether the organization has unintentionally made a single vendor's security record a single point of failure. Layering independent controls, such as zero trust access brokers and out-of-band monitoring, can limit fleet-wide exposure when one product family is compromised. Some organizations may also diversify perimeter platforms across critical asset classes, though the added configuration complexity, patching burden, and risk of misconfiguration must be weighed against the concentration benefit. Third-party risk programs should extend beyond software suppliers to logistics carriers and their OT posture, especially for routes and cargo types exposed to active geopolitical conflict.

Organizations should also bring geopolitical triggers into cyber risk planning. Events such as the reinstatement of a naval blockade [10] should prompt a review of threat assumptions for affected supply chains. Finally, operators should not wait for classification society or flag-state mandates. UR E26 in particular can serve as a reference baseline for existing ships even though it is mandatory only for new builds, and E27 can inform requirements placed on system suppliers [13]. Voluntary alignment may strengthen an operator's position in insurer and charterer due-diligence reviews.

CSA Resource Alignment

CSA's **Zero Trust Guidance for Critical Infrastructure** [14] is a directly applicable published resource. It applies zero trust principles to OT and ICS environments, including defining protect surfaces around physical processes, mapping transaction flows, and building microsegmentation that does not rely on a single perimeter. The FortiGate-to-OT pivot reported in this campaign is the failure mode that guidance is designed to prevent. A vessel's propulsion, steering, and cargo control systems are natural protect surfaces, and a zero trust architecture would require that compromise of the IT perimeter not translate into OT reachability. CSA's **Zero Trust Microsegmentation Guidance** [18] complements it with vendor-neutral guidance on implementing segmentation across IT, OT, IoT, cloud, edge, and agentic AI environments, which speaks directly to the onboard segmentation failures described above.

CSA's **Zero Trust Guidance for IoT** [15] and the **IoT Security Controls Framework v3** [16] address the device-level side of the problem. Shipboard networks contain the unmanaged, long-lived, network-connected devices those publications are designed for, including sensors, controllers, satellite terminals, and the "unexpected connected devices" CyberOwl reports finding aboard ships [4]. The IoT framework's

controls for asset inventory, credential management, firmware update, and secure remote access map directly onto the short-term mitigations above. The zero trust guidance for IoT offers a model for device identity and least-privilege connectivity where devices cannot host traditional agents.

The **AI Controls Matrix (AICM) v1.1** [17] provides the governance layer for organizations that deploy AI-driven monitoring, analytics, or autonomous functions on top of maritime and OT infrastructure. Its Infrastructure and Virtualization Security (IVS), Identity and Access Management (IAM), Threat and Vulnerability Management (TVM), and Supply Chain Management, Transparency, and Accountability (STA) domains together cover patching of edge infrastructure, credential hygiene, and third-party oversight. They also address the integrity of data feeding AI systems, which this campaign shows can be undermined at the network edge.

References

[1] McLaughlin, Jenna. "U.S. government investigates Iranian ties to as many as 50 hacked commercial vessels." NPR, November 24, 2026.

[2] Baran, Guru. "Hackers Exploit Fortinet Flaws to Breach Commercial Ships and Access Control Networks." Cyber Security News, November 25, 2026.

[3] Tamilselvan. "FBI and US Coast Guard Board Two Ships After Suspected Cyberattacks Compromise Vessel Networks." Cyber Press, November 26, 2026.

[4] Holt, Sean M. "When the Hacker Comes Aboard." The Maritime Executive, September/October 2026 (posted online November 22, 2026).

[5] Suciu, Peter. "Hackers Targeted a Supertanker. Could Ships Be the Next Critical Infrastructure Threat?" ClearanceJobs, September 18, 2026.

[6] Mallory. "U.S. Investigates Reported Cyberattacks on Up to 50 Cargo Ships and Tankers." Mallory (news aggregation, citing Wall Street Journal reporting), first seen November 24, 2026.

[7] Cybersecurity and Infrastructure Security Agency. "CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure." CISA, June 18, 2026.

[8] Paganini, Pierluigi. "CISA Warns of Active Exploitation Following FortiBleed Leak." Security Affairs, June 20, 2026.

[9] Paganini, Pierluigi. "Lab Dookhtegan hacking group disrupts communications on dozens of Iranian ships." Security Affairs, August 30, 2025.

[10] Wikipedia. "2026 United States naval blockade of Iran." Wikipedia, revision of November 27, 2026, accessed November 28, 2026.

[11] Canadian Centre for Cyber Security, with ASD's ACSC, CISA, NSA, NCSC-UK, and NCSC-NZ. "Security Considerations for Edge Devices (ITSM.80.101)." Canadian Centre for Cyber Security, February 2025.

[12] U.S. Coast Guard. "Cybersecurity in the Marine Transportation System (Final Rule)." Federal Register, January 17, 2025.

[13] International Association of Classification Societies. "Unified Requirements: E (Electrical and Electronic Installations), including UR E26 and E27." IACS, accessed November 28, 2026.

[14] Cloud Security Alliance. "Zero Trust Guidance for Critical Infrastructure." CSA, October 2024.

[15] Cloud Security Alliance. "Zero Trust Guidance for IoT." CSA, May 2025.

[16] Cloud Security Alliance. "IoT Security Controls Framework v3." CSA, April 2022.

[17] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, June 2026.

[18] Cloud Security Alliance. "Zero Trust Microsegmentation Guidance." CSA, 2026.